Technische und organisatorische Maßnahmen

Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

Zutrittskontrolle	Kein unbefugter Zutritt zu Datenverarbeitungs- anlagen.	• Sicherheitsschlösser • Schlüsselregelung (Schlüsselausgabe / -rückgabe) • Kontrollgang bei Verlassen des Standortes • Besucher und Dienstleister werden begleitet • Videoüberwachung des Außenbereichs
Zugangskontrolle	Keine unbefugte Systembenutzung.	• Authentifikation mit Benutzername und Passwort / Key-Verfahren • Rechte- und Rollenkonzept (Need 2 know-Prinzip) • Vorgaben für Passwörter und Passwort-Änderung • Sicherheitsschlösser • Schlüsselregelung (Schlüsselausgabe / -rückgabe) • Besucher und Dienstleister werden begleitet • Verschlüsselung von mobilen Datenträgern • Einsatz von Antivirensoftware • Einsatz von Firewalls
Zugriffskontrolle	Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems.	• Rechte- und Rollenkonzept (Need 2 know-Prinzip) • Anzahl der Administratoren auf das notwendigste reduziert • Verschlüsselung von mobilen Datenträgern • Vorgaben für Passwörter und Passwort-Änderung • Ordnungsgemäße Vernichtung von Datenträgern und Medien (z.B. Schredder)
Trennungskontrolle	Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken	• Trennung von Lokal, Sandbox, Development und Produktion (Live) • Trennung von Netzwerken VPCs (Virtual Private Clouds) • Rechte- und Rollenkonzept (Need 2 know-Prinzip) • Logische Mandantentrennung

	erhoben wurden.	
Pseudonymisierung	Personenbezogene Daten in einer Weise verarbeiten, dass diese ohne zusätzliche Informationen nicht zugeordnet werden können	• Nutzung von Pseudonymisierung wo möglich (u.a. bei Weitergabe) • Geeignete Wahl der Pseudonymisierungsschlüssel
Verschlüsselung	Klartext durch Schlüssel in nicht lesbaren Geheimtext umwandeln	• Geeignete Wahl der Verschlüsselung • Zusätzliche Verschlüsselung von Backups und Snapshots • Automatische Protokollierung der Schlüsselnutzung • Zugriffssteuerung (Need 2 know-Prinzip) • Gesicherte und ausfallsichere Schlüssel-Verwaltung

Integrität (Art. 32 Abs. 1 lit. b DSGVO)

Weitergabekontrolle	Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport.	• Abholung und Versand von eMails über gesicherte Verbindung (IMAPS, STMPS, STARTTLS, SSL) • Sichere Transportwege (z.B. https)
Eingabekontrolle	Feststellung, ob und von wem	• Protokollierung der Eingabe, Änderung und Löschung von Daten • Dokumentation von Vergabe und Entzug von Rechten

	personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt worden sind.	

Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

Verfügbarkeitskontrolle	Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust	• Redundante Internetverbindung • Einsatz von Antivirensoftware • Einsatz von Firewalls
Wiederherstellbarkeit	(Art. 32 Abs. 1 lit. c DSGVO)	• Erstellen eines Notfallplans • Nutzung von Backups und Snapshots • Nutzung virtueller Maschinen mit Offsitesicherung • Wartungsverträge mit geeigneter Reaktionszeit

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 DSGVO)

Datenschutz-Management		• Bestellung eines Datenschutzbeauftragten • Einsatz von Datenschutzkoordinatoren • Verzeichnis von Verarbeitungstätigkeiten • Datenschutzfolgeabschätzungen • Schulungsmaßnahmen / Sensibilisierungsmaßnahmen mit Nachweis • Verpflichtung auf Vertraulichkeit der Mitarbeiter • Definierte und dokumentierte Prozesse • Arbeitsanweisungen / Policies mit Datenschutzhintergrund • Regelmäßige Reviews der technischen & organisatorischen Maßnahmen

Incident-Response-Management		• Definition von Zuständigkeiten und Verantwortlichkeiten für Vorfälle (z.B. Vorfallteam) • Definierter Meldeprozess • Definierte Maßnahmen für relevante und denkbare Vorfälle • Definierte Eskalationswege • Aktuelle Melde- und Kontaktlisten • Prüfungsprozess für gemeldete Vorfälle und anschließender Risikoklassifizierung wenn zutreffend • Vorbereitete Reaktionen auf den Vorfall (Kommunikation wie auch technische Maßnahmen) • Reflektion und Nachbereitungsprozess um aus Vorfällen zu lernen
Datenschutzfreundliche Voreinstellungen	(Art. 25 Abs. 2 DSGVO)	• Prozess zur Sicherstellung von Privacy by Design bei Änderungen • Prozess zur Sicherstellung von Privacy by Default bei Änderungen
Auftragskontrolle	Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge	• Verpflichtung der MA auf das Datengeheimnis • Formal gestellter Datenschutzbeauftragter • AVV's und rechtliche Vertragsregelungen mit Sub-Dienstleistern • Schriftliche Weisungen an definierte Personen (je nach Anliegen)

	Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.	